National Infrastructure Protection Center CyberNotes

Issue #2001-24 *December 3, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between November 14 and November 28, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Acme Software[1]	Unix	thttpd 1.95-2.22	A buffer overflow vulnerability exists when thttpd attempts to decode the user name and password, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	thttpd Basic Authentication Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Allaire[2]	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1	A vulnerability exists due to the improper handling of malformed URLs, which could let a malicious user obtain sensitive information.	For workaround, see Macromedia Product Security Bulletin (MPSB01-13) located at: http://www.allaire.com/handlers/index.cfm?ID=22236&Method=Full	JRun Web Root Directory Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] Securiteam, November 25, 2001.
[2] Macromedia Product Security Bulletin, MPSB01-13, November 27, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Allaire[3]	Windows 95/98/NT 4.0/2000, Unix	JRun 2.3.3, 3.0, 3.1	A vulnerability exists when a specially crafted request is submitted for a non-existent .shtml file along with a known file, which could let a malicious user obtain sensitive information and execute arbitrary Java servlets.	For workaround, see Macromedia Product Security Bulletin (MPSB01-12) located at: http://www.allaire.com/handlers/index.cfm?ID=22235&Method=Full	JRun SSI Arbitrary File Source Disclosure	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Audio galaxy[4]	Multiple	Audiogalaxy	A vulnerability exists because the account name and information is stored in plaintext within a cookie, which could let a malicious user gain access to the account.	No workaround or patch available at time of publishing.	Audiogalaxy Plaintext Password Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Bharat Mediratta[5]	Multiple	Gallery 1.1-1.2.2	A Directory Traversal vulnerability exists due to insufficient validation of user-supplied input, which could let a malicious user view sensitive information.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=7130&release_id=62216	Gallery Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Caldera[6]	Unix	OpenUnix 8.0; UnixWare 7.1.0, 7.1.1	A buffer overflow vulnerability exists in the /usr/bin/X11/xlock program, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://stage.caldera.com/pub/security/openunix/CSSA-2001-SCO.34/xcontrib_801.pkg	XLock Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Cisco Systems[7]	Multiple	IOS 11.2P, 11.3T, 12.0XA-XE, 12.0XG, 12.0X, 12.0K, 12.0XM, 12.0XQ, 12.0XR, 12.0XV, 12.0T, 12.1YE, 12.1YF, 12.1YB, 12.1YC, 12.1XB, 12.1XC, 12.1XF-XM, 12.1XP, 12.1XT, 12.1, 12.1E, 12.1T, 12.2, 12.2DD, 12.2T, 12.2XD, 12.2XE, 12.2XH-12.2XK, 12.2XQ	A vulnerability exists in the Firewall Feature set (also known as Context Based Access Control and Cisco Secure Integrated Software), which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.cisco.com	Cisco Context Based Access Control Protocol Check Bypassing	Medium	Bug discussed in newsgroups and websites.

[3] Macromedia Product Security Bulletin, MPSB01-12, November 27, 2001.
[4] Bugtraq, November 27, 2001.
[5] Bugtraq, November 18, 2001.
[6] Caldera Security Advisory, CSSA-2001-SCO.34, November 16, 2001.
[7] Cisco Security Advisory, November 28, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Citrix[8]	Windows NT 4.0/2000	MetaFrame for Windows 2000 1.8 & NT 4.0 TSE 1.8	A vulnerability exists in the ICA protocol, which could let a malicious user have a false IP address logged.	No workaround or patch available at time of publishing.	MetaFrame False IP Address	Medium	Bug discussed in newsgroups and websites.
Cray[9]	Multiple	UNICOS/mk 2.0.5.54	A format string vulnerability exists in 'nqsdaemon,' which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	UNICOS NQS Daemon Format String	**High**	Bug discussed in newsgroups and websites.
Francisco Burzi[10]	Multiple	PHP-Nuke 5.1, 5.2., 5.3.1	A vulnerability exists when a user authenticates because a cookie is created which includes the account name and password, which could let a malicious user gain unauthorized access.	No workaround or patch available at time of publishing.	PHP-Nuke Weak Encryption In User Cookie	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
GNU[11]	Multiple	Mailman 2.0, 2.0.1-2.0.3, 2.0.5-2.0.7	A cross-site scripting vulnerability exists, which could let a malicious user execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/mailman/mailman-2.0.8.tgz	GNU Mailman Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard[12]	Unix	HP-UX 10.01, 10.10, 10.20, 11.0, 11.11	A vulnerability exists in the 'Rlpdaemon,' which could let a remote malicious user execute arbitrary code with superuser privileges.	Patch available at: PHCO_25107, PHCO_25108, PHCO_25109, PHCO_25110, PHCO_25111 http://itrc.hp.com/	HP-UX Remote Line Printer Daemon Logic Flaw CVE Name: CAN-2001-0817	**High**	Bug discussed in newsgroups and websites.
Home-Of-Linux.org[13]	Unix	GNOME libgtop_daemon 1.0.12	A format string vulnerability exists in the 'libgtop_daemon,' which could let a remote malicious user execute arbitrary code.	Update available at: http://freshmeat.net/redir/libgtop/5658/url_tgz/libgtop-1.0.13.tar.gz	Gnome libgtop_daemon Remote Format String	**High**	Bug discussed in newsgroups and websites.
HyperMail[14]	Unix	HyperMail 2.0.0-2.1.2	A vulnerability exists because HyperMail can be used to create arbitrary files that have arbitrary extensions, which could let a malicious user execute arbitrary SSI commands.	Upgrade available at: http://www.hypermail.org/dist/hypermail-2.1.3.tar.gz	HyperMail Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
IBM[15]	Unix	Informix SQL 7.31.UC5, 9.20.UC2	A Directory Traversal vulnerability exists in the Web DataBlade Module, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Informix SQL Web DataBlade Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[8] Xato Security Advisory, XATO-112001-01, November 14, 2001.
[9] Bugtraq, November 28, 2001.
[10] Bugtraq, November 21, 2001.
[11] CGISecurity Advisory #7, November 28, 2001.
[12] Hewlett-Packard Company Security Bulletin, HPSBUX0111-176, November 20, 2001.
[13] Intexxia(C) Security Advisory, ID #1048-261101, November 27, 2001.
[14] qDefense Advisory Number QDAV-2001-11-1, November 19, 2001.
[15] Bugtraq, November 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Imatix[16]	Windows 95/98/NT 4.0/2000	Xitami 2.4, 2.5	A vulnerability exists in the 'default.aut' file, which could let a malicious user obtain admin authentication information and execute commands as root.	No workaround or patch available at time of publishing.	Xitami Administrator Plain Text Password Storage	**High**	Bug discussed in newsgroups and websites.
Intel Corporation[17]	Multiple	High-bandwidth Digital Content Protection 1.0	High bandwidth Digital Content Protection (HDCP) is a system for preventing access to plaintext video data sent over Digital Visual Interface (DVI). Any technique that allows access to the plaintext data is considered breaking the system. This could let a malicious user authenticate as an arbitrary device.	No workaround or patch available at time of publishing.	HDCP Authentication Linear Relation Between Keys	Medium	Bug discussed in newsgroups and websites.
Legato[18]	Multiple	NetWorker 6.0	A vulnerability in the in the authentication scheme, which could let a remote malicious user bypass the authentication procedure.	Update available at: http://portal2.legato.com/resources/downloads/networker.cfm	NetWorker Reverse DNS Authentication	Medium	Bug discussed in newsgroups and websites.
Microsoft[19]	Windows 95/98/ME/ NT 3.5.1/4.0/ 2000	Internet Explorer 5.5SP1 & SP2, 5.0, 6.0	A vulnerability exists when the Microsoft Internet Explorer patch Q312461 is installed because the 'HTTP_USER_AGENT' variable reveals the user agent name along with operating system information, which could assist a malicious user in locating unpatched browsers and launching attacks against them.	MS Internet Explorer Patch Q312461 is the source of this issue since it reveals whether or not it exists on a system via HTTP_USER_AGENT, however users should ensure that the patch is installed to prevent exploitation of the issues discussed in Microsoft Security Bulletin MS01-055. Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-055.asp	Microsoft Internet Explorer Patch Q312461 Existence	Medium	Bug discussed in newsgroups and websites.

[16] Vapid Labs, 11232001-02, November 23, 2001.
[17] SecurityFocus, November 20, 2001.
[18] Securiteam, November 26, 2001.
[19] Bugtraq, November 19, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[20]	Windows 95/98/ME/ NT 3.5.1/4.0/ 2000	Internet Explorer 4.0 for Windows 95/98/NT 4.0, 4.0.1SP2, 4.0.1 for Windows 95/98/NT 4.0, 4.1 for Windows 95/98/NT 4.0, 5.5, 5.5SP1 & SP2, 6.0	A vulnerability exists when providing a password in IE, which could let a malicious user differentiate between alphanumeric and non-alphanumeric characters used in a password.	No workaround or patch available at time of publishing.	Microsoft Internet Explorer Password Character Determination	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[21]	Windows NT 4.0/2000	Windows Media Player 6.4, 7, 7.1, Media Player for Windows XP	An unchecked buffer vulnerability exists in the Advanced Streaming Format (ASF) media format, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-056.asp	Windows Media Player .ASF Processor Contains Unchecked Buffer	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[22]	Unix	Linux kernel 2.4-2.4.11	A Denial of Service vulnerability exists when a second instance of the kernel is executed from the command line.	Contact your vendor and upgrade to a 2.4.12 or later kernel	VMLinux Arbitrary Kernel Execution Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[23, 24, 25, 26, 27]	Unix	David Madore ftpd-BSD 0.3.2, 0.3.3; Washington University wu-ftpd 2.5.0, 2.6.0 2.6.1	A heap corruption vulnerability exists in the implementation of file globbing included in Wu-Ftpd, which could let a remote malicious user execute arbitrary code.	**SuSE:** ftp://ftp.suse.com/pub/suse/ **RedHat:** ftp://updates.redhat.com/ **Caldera:** ftp://ftp.caldera.com/pub/updates/ **Immunix:** http://download.immunix.org/ImmunixOS/7.0/updates/ **Conectiva Linux:** ftp://atualizacoes.conectiva.com.br/	Wu-Ftpd File Globbing Heap Corruption CVE Name: CAN-2001-0550	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Netscape Communications[28]	MacOS 6.0.8-9.2.1, MacOS X 10.0-10.1	Netscape 4.77 Mac	A vulnerability exists when webpages viewed in Netscape are printed out that contain password fields, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Netscape For MacOS Password Field Printing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[20] Bugtraq, November 21, 2001.
[21] Microsoft Security Bulletin, MS01-056, November 19, 2001.
[22] Bugtraq, November 21, 2001.
[23] SuSE Security Announcement, SuSE-SA:2001:043, November 28, 2001.
[24] RedHat Security Advisory, RHSA-2001:157-06, November 26, 2001.
[25] Caldera International Security Advisory, CSSA-2001-041.0, November 28, 2001.
[26] Immunix OS Security Advisory, IMNX-2001-70-036-01, November 28, 2001.
[27] Conectiva Linux Security Announcement, CLA-2001:442, November 29, 2001.
[28] Bugtraq, November 21, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Network Solutions, Incorporated[29]	Unix	RWhoIsD 1.5, 1.5.1a, 1.5.2, 1.5.3, 1.5.5, 1.5.6, 1.5.7, 1.5.7.2	A format string vulnerability exists in the RWHOIS daemon, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	RWhoIsD System Log Format String	**High**	Bug discussed in newsgroups and websites.
OpenBSD[30]	Unix	OpenSSH 3.0, 3.0p1	A vulnerability exists in the way KerberosV authentication is handled, which could let a remote malicious user obtain unauthorized access.	Upgrade available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/	OpenSSH Kerberos Arbitrary Privilege Elevation	Medium	Bug discussed in newsgroups and websites.
Oracle Corporation[31]	Windows NT 4.0/2000, Unix	Oracle9iAS Web Cache 2.0.0.2 NT, 2.0.0.2, 2.0.0.1	A remote Denial of Service vulnerability exists due to the way unexpected queries to the Web Cache software are handled.	Upgrade available at: http://metalink.oracle.com	Oracle9iAS Web Cache HTTP Content Header Denial Of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Patrick Schemitz[32]	Unix	AutoNice Daemon 1.0.0-1.0.4	A format string vulnerability exists in the AutoNice Daemon (AND), which could let a malicious user execute arbitrary code.	Upgrade available at: http://and.sourceforge.net:/and-1.0.5.tar.gz	AutoNice Daemon Program Name Format String	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat [33]	Unix	Stronghold 2.3, 2.4, 3.0	A vulnerability exists in the default installation, which could let a remote malicious user obtain sensitive information.	Installing Stronghold/3.0 build 3015 will solve the problem.	Stronghold Secure Web Server Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Sun Microsystems, Inc.[34]	Unix	Net Dynamics 4.0, 4.1, 4.1.2, 4.1.3, 5.0	A vulnerability exists because a previously generated session ID to that of a legitimate logged in user remains valid for that account for 15 seconds after login, which could let a malicious user hijack the user's account.	No workaround or patch available at time of publishing.	NetDynamics Session ID Hijacking	Medium	Bug discussed in newsgroups and websites.
SuSE[35]	Unix	Linux 6.4, 6.4ppc & alpha, 7.0, 7.0ppc & alpha, 7.1x86, ppc & alpha, 7.2	A format string and buffer overflow vulnerability exists in the 'pmake' program, which could let a malicious user execute arbitrary code with root privileges.	Update available at: ftp://ftp.suse.com/pub/suse/	Berkeley Parallel Make Buffer Overflow and Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
SuSE[36]	Unix	Linux 7.2, 7.3	A vulnerability exists in several of the SuSEHelp CGI scripts, which could let a remote malicious user execute arbitrary code.	Patch available at: ftp://ftp.suse.com/pub/suse/i386/update/	Linux SuSEHelp CGI Insecure Temporary File	**High**	Bug discussed in newsgroups and websites.

[29] NetGuard Security Team alert7, November 22, 2001.
[30] Bugtraq, November 19, 2001.
[31] Securiteam, November 27, 2001.
[32] Intexxia(C) Security Advisory, ID #1047-231101, November 26, 2001.
[33] VIGILANTE-2001002, November 23, 2001.
[34] NMRC Advisory, November 26, 2001.
[35] Securiteam, November 24, 2001.
[36] SuSE Security Announcement, SuSE-SA:2001:041, November 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
TWIG[37]	Multiple	TWIG 2.6-2.7.4	A vulnerability exists because the account name and password are stored in an unencrypted cookie, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	TWIG Plaintext Password in Cookies Under Default Installation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Xircom[38]	Multiple	Rex 6000	A vulnerability exists in the way the pin code is transferred from the PDA to the Rextoola application, which couldlet a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Rex 6000 Password Retrieval	Medium	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 20 and November 29, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 8 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
November 29, 2001	Comphack.c	A remote exploit script for Compaq Insight Manager.
November 28, 2001	Mognet-1.13.tar.gz	A GPL'd libpcap/jpcap 802.11b sniffer/analyzer written in Java that is display-optimized for use on handheld devices like the iPaq.
November 27, 2001	Wu-ftpd.2.6.0.rfp	Details and source diffs for the wu-ftpd v2.6.1 remote overflow vulnerability.

[37] Bugtraq, November 28, 2001.
[38] Bugtraq, November 23, 2001.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
November 26, 2001	Steghide-0.4.2.tar.gz	A steganography program that hides bits of a data file in some of the least significant bits of another file in such a way that the existence of the data file is not visible and cannot be proven. Steghide is designed to be portable and configurable and features hiding data in bmp, wav and au files, blowfish encryption, MD5 hashing of passphrases to blowfish keys, and pseudo-random distribution of hidden bits in the container data.
November 24, 2001	Pmexpl.c	Script which exploits the Berkeley Parallel Make Buffer Overflow and Format String vulnerability.
November 24, 2001	Winfingerprint040.zip	Advanced remote windows OS detection tool.
November 21, 2001	Cgixp.exe	A remote exploit for Webcart v8.4 and several Unicode vulnerabilities.
November 21, 2001	Write.c	Proof of concept code for the Solaris 2.6 and 2.7 (SPARC) "write" buffer overflow vulnerability.

Trends

Probes/Scans:

- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**
- **CERT/CC is receiving reports of increased scanning activity for the SSH service (22/tcp). For more information, see CERT® Incident Note IN-2001-12, located at: http://www.cert.org/incident_notes/IN-2001-12.html.**

Other:

- **NIPC has learned about vulnerability in versions of the Washington University File Transport Protocol Daemon (WU-FTPD) that could lead to an attacker gaining surreptitious access to sensitive information. For more information, see NIPC ADVISORY 01-027 located at: http://www.nipc.gov/warnings/advisories/2001/01-027.htm.**
- **NIPC has reason to believe that the potential for future DDoS attacks is high. Protesters have indicated they are targeting web sites of the U.S. Department of Defense and organizations that support the critical infrastructure of the United States. For more information, see NIPC ADVISORY 01-026 located at: http://www.nipc.gov/warnings/advisories/2001/01-026.htm.**
- **The National Infrastructure Protection Center (NIPC) continues to observe hacking activity targeting the e-commerce or e-finance/banking industry. For more information, see NIPC ADVISORY 01-023 located at: http://www.nipc.gov/warnings/advisories/2001/01-023.htm. The most prevalent exploit being used to gain access to targeted systems is the Unicode vulnerability found in the Microsoft Internet Information Services (IIS) web server software, http://www.microsoft.com/technet/treeview/default.asp?url=/technet.security/bulletin/MS00-086.asp.**
- **CERT/CC has received multiple reports of systems being compromised via the CRC-32 compensation attack detector vulnerability. For more information, see CERT® Incident Note IN-2001-12, located at: http://www.cert.org/incident_notes/IN-2001-12.html.**
- **CERT has released a statement concerning multiple vulnerabilities in several implementations of the line printer daemons of several types of systems. These holes would allow intruders to gain root privileges and launch Denial of Service attacks through IBM AIX line printers, FreeBSD, netBSD, openBSD and Hewlett-Packard Co. HP-UX line printers. For more information, see CERT Advisory CA-2001-30, located at: http://www.cert.org/advisories/CA-2001-30.html.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

PE_JIMMY.B (Alias: JIMMY.B) (File Infector Virus): This polymorphic virus infects PE EXE files on Windows 9x/ME/NT/2000 systems. To infect, it appends its code to the host file. It does not have a destructive payload.

VBS.Snav (Visual Basic Script Worm): This virus is written using the Visual Basic Scripting (VBS) language. When the virus is executed, it copies itself as Readme.vbs to all folders on all local and network drives. The virus stops executing when an error occurs, such as not having the required permissions to create files on network drives.

W32/Badtrans-B (Win32 Worm): This is a worm that uses MAPI to spread. The worm arrives in an e-mail message with no message text. The attachment filename is randomly generated from three parts. If the attached file is run, it copies itself into the Windows system directory with the filename KERNEL32.EXE and changes the registry key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

so that the worm runs the next time Windows is started. The worm also drops a file named kdll.dll, which is the password stealing Trojan, Troj/PWS-AV.

W32.Eira.57344@mm (Aliases: W32/Eira.A@mm, I-Worm.Quamo) (Win32Worm): This is an Internet worm which carries a file-overwriting payload. The file name of this worm suggests that it is a demo of the Quake4 game, but it is not.

W97M.Twopey.B (Word 97 Macro Virus): This is a macro virus that infects Word documents and templates. Infected documents may have properties the following properties:

Author = "OPEY A." 'GREETINGS TO ALL FILIPINO PROGRAMMERS !!!
Title = "OpeY 2k1 version - Philippines"

WM97/Ethan-EN (Word 97 Macro Virus): This virus is a member of the WM97/Ethan Word macro virus family with no malicious payload.

WM97/Marker-JX (Word 97 Macro Virus): This virus is a variant of the WM97/Marker-A virus. It creates a file called JON.HTML in the Windows directory (usually C:\WINDOWS under Windows 95/98 or C:\WINNT under Windows NT), and reconfigures Internet Explorer's desktop to use this HTML file. The virus deletes all .DOC files and .DOT files in the Word application startup directory, although documents are not normally stored in this directory. The virus also changes the user settings of Word, including changing the ownership of Word to JonMMx 2000. These settings can be corrected in the Tools|Options|User Information menu within Microsoft Word.

W97M/Marker.JY (Word 97 Macro Virus): This virus infects Word 97 documents and templates. This is a class module virus for Word 97 documents. It is able to replicate in the SR-1 and above releases of Word 97. It will turn off the macro warning feature of Word 97. It consists of a module within the class stream named "ThisDocument" and also another module Hider831912. The virus will cause the following message to be displayed. "Configuration error, please reinstall Microsoft Word" when the user tries to access Tools/Macro or Tools/Macro/Visual Basic Editor.

WM97/Marker-JZ (Word 97 Macro Virus): This virus is a corrupted but viable variant of the WM97/Marker-C Word macro virus. Whenever a document is closed, the virus attempts to FTP user information from Word to the Codebreakers website and appends this information to the bottom of the macro as comments.

WORM_ALIZ.A (Aliases: ALIZ.A, W32.Aliz.Worm, W32/Aliz@MM, W32/Aliz, W32/Aliz.A, TROJ_ALIZ.A) (Worm): This non-destructive, mass-mailing worm propagates copies of itself via e-mail. It arrives as an embedded executable file, WHATEVER.EXE. It does not require the e-mail receiver to open the attachment for it to execute. It uses a known vulnerability in Internet Explorer-based e-mail clients (Microsoft Outlook and Microsoft Outlook Express) to automatically execute the file attachment. This is also known as Automatic Execution of Embedded MIME type. The infected e-mail contains the executable attachment registered as content-type of audio/x-wav so that when recipients view the infected e-mail, the default application associated with audio files is opened. The embedded EXE file cannot be viewed in Microsoft Outlook.

WORM_CBLAD.A (Aliases: CBLAD.A, W32.Cblade.Worm, W32/Cblade.worm) (Worm): This memory-resident Internet worm uses a known MS SQL 7 server vulnerability to propagate. The vulnerability allows the execution of a command shell on systems with the Systems Administrator account's password set as empty by default. This worm is also capable of performing a Distributed Denial of Service Attack (DDoS Attack) on target systems. It instructs the exploited MS SQL servers to connect to an IRC server to receive instructions from the attacker.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Adshow	N/A	CyberNotes-2001-17
AOL.PWSteal.86016	N/A	CyberNotes-2001-14
Artic	0.6 beta	CyberNotes-2001-14
Asylum	N/A	CyberNotes-2001-18
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	N/A	CyberNotes-2001-14
Backdoor.Darkirc	N/A	CyberNotes-2001-15
Backdoor.Darksun	N/A	CyberNotes-2001-21
Backdoor.Destiny	N/A	CyberNotes-2001-21
Backdoor.G_Door	N/A	CyberNotes-2001-18
Backdoor.IRC.Critical	N/A	CyberNotes-2001-19
Backdoor.IRC.Flood	N/A	CyberNotes-2001-16
Backdoor.KWM	N/A	CyberNotes-2001-21
Backdoor.Litmus	N/A	CyberNotes-2001-21
Backdoor.MiniCommander:	N/A	CyberNotes-2001-16
Backdoor.Oblivion	N/A	CyberNotes-2001-22
Backdoor.Penrox	N/A	CyberNotes-2001-17
Backdoor.Slackbot.B	N/A	CyberNotes-2001-21
Backdoor.Teste	N/A	CyberNotes-2001-16
Backdoor.Way	N/A	CyberNotes-2001-18
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	N/A	CyberNotes-2001-14
Backdoor-QV	N/A	CyberNotes-2001-14

Trojan	Version	CyberNotes Issue #
Backdoor-QZ	N/A	CyberNotes-2001-14
BAT.Black	N/A	CyberNotes-2001-11
Bat.FAGE.1482	N/A	CyberNotes-2001-15
Bat.Hexvirus.1414	N/A	CyberNotes-2001-15
Bat.PG94.3964	N/A	CyberNotes-2001-15
BAT_FORMATC.K	N/A	CyberNotes-2001-13
CodeRed II	II	CyberNotes-2001-16
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
DonaldD.Trojan.C	N/A	CyberNotes-2001-19
EIC.Trojan	N/A	CyberNotes-2001-14
Girlgif.Trojan	**N/A**	**Current Issue**
Goga	N/A	CyberNotes-2001-12
Gribble	N/A	CyberNotes-2001-19
HackTack	N/A	CyberNotes-2001-18
IRC/FinalBot	N/A	CyberNotes-2001-18
J_PWS.REDNECK	N/A	CyberNotes-2001-22
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.Alert.Trojan	N/A	CyberNotes-2001-19
JS.Seeker.B	N/A	CyberNotes-2001-18
JS_EXCEPTION.C	N/A	CyberNotes-2001-21
JS_EXCEPTION.GEN	**N/A**	**Current Issue**
JS_OFFENSIVE.A	N/A	CyberNotes-2001-17
JS_SEEKER.W:	N/A	CyberNotes-2001-23
JS_ZOPA.A	N/A	CyberNotes-2001-14
KillMBR.g	N/A	CyberNotes-2001-16
Lil Witch FTP	1.0	CyberNotes-2001-19
MoSucker	N/A	CyberNotes-2001-23
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
Phoenix	2.1.28	CyberNotes-2001-18
Phreak	N/A	CyberNotes-2001-22
PWS.Cain.dr	N/A	CyberNotes-2001-19
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
QDel172	N/A	CyberNotes-2001-17
Remote Shell Trojan	N/A	CyberNotes-2001-19
SennaSpy Generator	N/A	CyberNotes-2001-13
Septer.Trojan	N/A	CyberNotes-2001-21
Shake.Trojan	N/A	CyberNotes-2001-20
StealVXS	N/A	CyberNotes-2001-17
Troj/PsychwardB	N/A	CyberNotes-2001-14
Troj/PWS-AV	**N/A**	**Current Issue**
Troj/Slack	N/A	CyberNotes-2001-14
TROJ_ALLGRO.A	N/A	CyberNotes-2001-17
TROJ_ANSET.B	N/A	CyberNotes-2001-22
TROJ_APOST.A	N/A	CyberNotes-2001-18
TROJ_BADY	N/A	CyberNotes-2001-15
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_CAFEIN111.A	N/A	CyberNotes-2001-14
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DSNX.A	N/A	CyberNotes-2001-17
TROJ_HAI.A	N/A	CyberNotes-2001-17
TROJ_ICMPBOMB.A	N/A	CyberNotes-2001-17
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_INVALID.A	N/A	CyberNotes-2001-18
TROJ_IRC_NETOL.A	N/A	CyberNotes-2001-14
TROJ_JESTRO.A	N/A	CyberNotes-2001-20

Trojan	Version	CyberNotes Issue #
TROJ_KALM.A.SVR	N/A	CyberNotes-2001-21
TROJ_KEYLOG.25	N/A	CyberNotes-2001-17
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MODNAR.A	N/A	CyberNotes-2001-17
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MUSTARD.A	N/A	CyberNotes-2001-19
TROJ_NEWPIC.A	N/A	CyberNotes-2001-17
TROJ_NEWSAGENT.A	N/A	CyberNotes-2001-16
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_OPTIX.SVR	N/A	CyberNotes-2001-17
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_RUSH.A	N/A	CyberNotes-2001-21
TROJ_SIRCAM.A	N/A	CyberNotes-2001-15
TROJ_SPYBOY.A	N/A	CyberNotes-2001-18
TROJ_UCON.A	N/A	CyberNotes-2001-21
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VOTE.A	A	CyberNotes-2001-19
TROJ_VOTE.B	B	CyberNotes-2001-20
TROJ_VOTE.C	C	CyberNotes-2001-20
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WHISTLER.A	N/A	CyberNotes-2001-19
TROJ_ZERAF.A	N/A	CyberNotes-2001-18
Trojan.Assault.10	10	CyberNotes-2001-15
Trojan.Bat.Live4:	N/A	CyberNotes-2001-16
Trojan.Billrus.Texto	N/A	CyberNotes-2001-14
Trojan.Diagcfg	N/A	CyberNotes-2001-15
Trojan.JS.Clid.gen	N/A	CyberNotes-2001-17
Trojan.JS.Cover	N/A	CyberNotes-2001-18
Trojan.Lornuke	N/A	CyberNotes-2001-14
Trojan.Offensive	N/A	CyberNotes-2001-17
Trojan.Pounds	N/A	CyberNotes-2001-18
Trojan.PSW.GIP	**N/A**	**Current Issue**
Trojan.Spy.KIM	N/A	CyberNotes-2001-23
Trojan.VBS.PWStroy	N/A	CyberNotes-2001-14
Trojan.VirtualRoot	N/A	CyberNotes-2001-16
Trojan.Xtratank	N/A	CyberNotes-2001-17
Trojan.Zeraf	N/A	CyberNotes-2001-17
Trojan.ZeroBoot	N/A	CyberNotes-2001-19
VBS.Alal	**N/A**	**Current Issue**
VBS.AutoExec.Trojan	N/A	CyberNotes-2001-16
VBS.Blank.A	N/A	CyberNotes-2001-14
VBS.Dayumi	N/A	CyberNotes-2001-22
VBS.Fiber.C	N/A	CyberNotes-2001-18
VBS.Masteal.Trojan	N/A	CyberNotes-2001-21
VBS.Natas	N/A	CyberNotes-2001-16
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Icon	N/A	CyberNotes-2001-18

Trojan	Version	CyberNotes Issue #
VBS.Trojan.Lariara	N/A	CyberNotes-2001-18
VBS.Zync.A	N/A	CyberNotes-2001-17
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.Delalot.Trojan	**N/A**	**Current Issue**
W32.DpBot.Trojan	N/A	CyberNotes-2001-22
W32.Elem.Trojan	**N/A**	**Current Issue**
W32.JavaKiller.Trojan	N/A	CyberNotes-2001-21
W32.Leave.B.Worm	N/A	CyberNotes-2001-14
W32.Whiter.Trojan	N/A	CyberNotes-2001-20
Y3K Rat	1.6	CyberNotes-2001-11
Zendown	N/A	CyberNotes-2001-22

Girlgif.Trojan: Girlgif.Trojan is a Trojan horse that usually is sent by a hacker using e-mail. The e-mail message has two attachments: Girl.exe and Girl.gif. The Girl.gif file is actually a .dll file, not a .gif file. Both of these files are packed using the Aspack utility. When Girl.exe is executed, it looks for the Girl.gif file in the same folder in which it resides. If it finds Girl.gif, it copies it to \Windows\System as Imnepr.dll. It then registers the Imnepr.dll file, and hooks the keyboard and Windows messages to track whatever you type or execute. The Trojan might track passwords that you use to log in to specific locations. Some of the tracked keyboard and Windows messages are written to the \Windows\System\Systems.dat file. The Systems data file is a log file that is created by the Trojan. The Trojan may then attempt to send this log file to a hacker's e-mail account in China; however, this e-mail account is not currently active.

JS_EXCEPTION.GEN (Aliases: Trojan.Seeker-based, HTML.VMExploit, JS.Exception.Exploit, EXCEPTION, EXCEPTION.GEN): This Java Script Trojan exploits security vulnerabilities in the Microsoft Virtual Machine. It allows a Java applet from a malicious Web site to execute any command on a visiting user’s machine. Some variants have destructive payloads such as modifying file associations, modifying the appearance of Internet Explorer, and downloading executable files.

Trojan.PSW.GIP: This Trojan belongs to the family of password-stealing Trojans. When run, the Trojan installs itself to the system, and while installing, copies itself to Windows, Windows system, Windows temporary, or Windows\RECYCLED directory and registers itself in the system registry auto-run section. The installed Trojan file name and target directory are optional. They are stored in encrypted form in the Trojan file at the file end. A malicious user may configure them before sending the Trojan to a victim machine, or before putting it on a Web site. The Trojan then registers itself in the system as a hidden application (service), and the Trojan process then is not visible in task list. Being active in the system, the Trojan periodically sends e-mail messages to its host (hacker's e-mail address, also is optional). The Trojan can download a file from a specified Internet site and registers it in the Registry auto-run key:

```
        HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce Welcome = TMP15F.EXE
```

It may drop a "decoy" component - a joke program, game, and other kind of attractive program. This is done to deceive a user and disguise the Trojan's installation by a decoy component.

Troj/PWS-AV: This Trojan is dropped by W32/Badtrans-B worm. It logs the user's keystrokes in order to gain privileged information such as passwords.

VBS.Alal: This is a Trojan horse that copies itself to the \Windows, \Windows\System, and Windows temporary folders. It overwrites all .txt and .doc files that it finds with a text message. It also creates a text file in the \Windows folder.

W32.Delalot.Trojan: This is a Trojan horse that starts itself as a service to run invisibly and then attempts to delete all files on drives C, D, E, F, and A, in that order.

W32.Elem.Trojan: This is a Trojan horse that arrives appearing to be a key generator for Windows XP. It may also be available from a file sharing application service named Kazaa. This Trojan is actually a Pklite package containing zero-byte files. Its purpose is to overwrite existing files with the zero-byte files.